broken-session-managment

1- login to your account with firefox and chrome
- change the password in firefox
- observe the account in chrome is still logged in and didn't logout
- Broken session Management
`

2- login to your account with firefox and chrome
- enable 2FA in firefox
- reload the page in chrome and observe session is still valid

3- login to your account and update anything
- intercept the request with burpsuite
- send the request to repeater
- logout from your account
- use the request in repater to update and if still valid (vulnerability)

4- ask for reset password
- don't click on the link reached you
- login with your username and password
- change the password of the email
- logout from your account and then use the link in step 1
- if still valid then (Vulnerability)

5-logout from your account
- click on (Alt+Left-arrow) button or <--
- observe the session and profile data is still found
- broken cache vulnerability

6- when updating email address
- check if OTP is sent to existing email not the new email
- broken function lead to verification bypass

7- create account with email A => victim
- update the email to B => hacker then verify it -> vierfy your account
- update email back to A => victim
- if shown as verified then vulnerability

8- verifiaction bypass
- account with victim@gmail.com => don't verify it

- update account email to hacker@gmail.com
- once you clicked the link , if verified victim@gmail.com then vuln

---

- 1 - بتسجل الاكونت ف اكتر من مكان
  - بتغير الباسورد
  - تشوف لسه مفتوح علي باقي الاجهزه ولا لا
  - لو لسه تبقي ثغره

- 2 - بتسجل الاكونت ف اكتر من مكان
  - بتفعل ال 2FA
  - تشوف لسه مفتوح علي باقي الاجهزه ولا لا
  - لو لسه تبقي ثغره

- 3 - بتسجل دخول ف اي موقع
  - بتغير اسمك مثلا وتوقف الطلب
  - تبعته لل Repeter وتسيبه
  - تعمل logout
  - ترجع لل Repeter
  - وتبعت الـ Request المفروض ال session تكون خلصت لو الـ Request اتبعت كدا ثغره

- 4 - بتعمل طلب تغير للباسورد
  - هيتبعتلك link علشان تغير الباسورد متستخدموش
  - سجل دخول عادي بالايميل والباس
  - غير الباس *المفروض الـ link يحصله expire*
  - اعمل logout
  - روح شوف الـ link لسه شغال ولا لا لو شغال تبقي ثغره

- 5 - اعمل logout

- 
- بتضغط علي زر الرجوع لو رجعك للاكونت تاني تبقي ثغره (broken cache vulnerability)

- 6 - لو جيت تغير الجيميل فالاكونت
  - كود هيجيلك علي الجيميل الجديد
  - الكود لو اتبعت علي الجيميل القديم كدا ثغره

- 7 - بتعمل اكونت جديد هيجيلك Link علشان تعمل Verfiy للاكونت
  - متعملوش Verfiy
  - بتخش تغير الجيميل تعمله و Verfiy
  - بعدها بترجع تغير الجيميل تاني بس للاكونت الاول اللي انت معملتوش Verfiy
  - لو لقيته معموله Verify تبقي كدا ثغره

- 8 - بتعمل اكونت متعملوش Verify
  - تبعمل update للجيميل وتعمله Verify
  - لو لقيت الاكونت الاول هوه اللي اتعمله Verify بتقي كدا ثغره